



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

July 8, 1997

**RECEIVED**

JUL - 9 1997

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

Mr. William F. Caton  
Acting Secretary  
Federal Communications Commission  
Room 222  
1919 M Street, N.W.  
Washington, D.C. 20554

DOCKET FILE COPY ORIGINAL

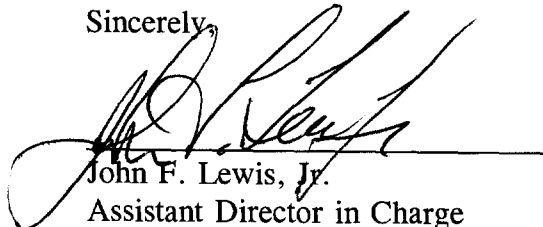
RE: In the Matter )  
Implementation of the )  
Telecommunications Act of 1996: )  
Telecommunications Carriers' Use of )  
Customer Proprietary Network Information )  
And Other Customer Information; )  
NOTICE OF PROPOSED RULEMAKING )

CC Docket 96-115

Dear Mr. Caton:

Enclosed for filing please find an original and four copies of the Comments of the Federal Bureau of Investigation in the above captioned matter.

Sincerely,

  
John F. Lewis, Jr.  
Assistant Director in Charge  
National Security Division

cc: Common Carrier Bureau  
International Bureau  
Wireless Telecommunications Bureau  
International Transcription services, Inc.  
International Reference Room, International Bureau  
Wireless Reference Room, wireless Telecommunications Bureau

No. of Copies made  
LIST ABOVE

044



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

Before the  
Federal Communications Commission  
Washington, D.C. 20554

RECEIVED

JUL - 9 1997

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

In the Matter of )  
Implementation of the )  
Telecommunications Act of 1996: )  
Telecommunications Carriers' Use of )  
Customer Proprietary Network Information )  
And Other Customer Information; )  
NOTICE OF PROPOSED RULEMAKING )

CC Docket 96-115

Comments of the Federal Bureau of Investigation

**Comment One:** The Federal Bureau of Investigation (FBI) believes that the Federal Communications Commission (FCC) should impose constraints on telecommunications carriers licensed by the FCC (hereafter, carriers) with regard to their current ability to store Customer Proprietary Network Information (CPNI) outside the United States and their ability to access, from outside the U.S., CPNI that is stored in the U.S., with regard to the CPNI of U.S. customers who only subscribe to domestic telecommunications services (Domestic Customers).<sup>1</sup> Specifically, the FBI believes that the FCC should mandate that the CPNI of Domestic Customers shall be exclusively stored in (accessible from) the United States. The FBI believes that distinct and deleterious national security, law enforcement, public safety, business-proprietary, and privacy concerns are raised when foreign-based storage of, or direct foreign access to, the CPNI of Domestic Customers is permitted.

**Comment Two:** The FBI believes that the concerns regarding foreign-based storage of, or direct foreign access to, the CPNI of Domestic Customers, although arguably more likely to arise with regard to foreign-based carriers, nevertheless logically would apply to all carriers

---

<sup>1</sup> For purposes of describing *customers who only subscribe to domestic telecommunications services (Domestic Customers)* as used in this Comment, we are referring to customers, both individuals and businesses, whose telecommunications service (and whose CPNI related to such service) is essentially intra-U.S. in nature. Such service would encompass conventional long distance service, including long distance service where international calls may be placed; but it would be distinguished from international service(s) provided pursuant to special contract or tariff arrangement for international services or similar volume discount arrangement.

since the harm to be avoided with regard to U.S. Governmental and customer interests is essentially identical regardless of whether the carrier is U.S. or foreign-based. Moreover, because important public safety, law enforcement, and national security concerns as well as subscriber business-proprietary and privacy concerns are at risk, the constraints proposed in this Comment should logically be applied without regard to the size or competitive circumstances of carriers. To wit, a carrier's "dominance," or lack thereof, is irrelevant to proper resolution of the concerns expressed here.

**Comment Three:** Foreign-based storage of, or direct foreign access to, the CPNI of Domestic Customers raises fundamental questions related to the efficacy of FCC regulations and other U.S. laws related to CPNI, particularly with regard to national security, law enforcement, public safety, business-proprietary, and privacy concerns. If foreign storage of, or direct foreign access to, such CPNI is permitted, on the one hand, the FCC's jurisdictional reach, its enforcement, audit, and inspection capabilities, etc. regarding carrier facilities, and activities conducted abroad, would be extremely doubtful both as a practical and legal matter; and, on the other hand, the laws and (or) the practices of the foreign country where the CPNI is stored, or from which it can be electronically accessed, could effectively nullify and supersede provisions of U.S. law related to CPNI. Stated differently, although FCC rules and regulations regarding CPNI would be preemptive within the U.S., and control CPNI exclusively, the same cannot be said when the jurisdictional reach and laws of another country are implicated through foreign-based storage or foreign-based direct access.<sup>2</sup> Moreover, the prospect of direct foreign access to the CPNI of U.S. Domestic Customers would have the unintended effect of seriously undermining, legally and practically, important U.S. Governmental, business-proprietary, and privacy-based protections that are afforded to CPNI under international and bilateral treaties (e.g., Mutual Legal Assistance Treaties (MLATs))<sup>3</sup> and other international legal assistance procedures (e.g., Letters Rogatory).

---

<sup>2</sup> We note that the FCC in the instant proposed rulemaking has chosen to articulate (under Section III A, "Scope of Commission's Authority") its preemption in the area of CPNI. The Commission goes on to state that the Telecommunications Act of 1996 " 'balance[s]' both competitive and consumer privacy interests with respect to CPNI." In this Comment, we argue that the preservation of privacy interests, *inter alia*, would be illusory if foreign-based storage of, or direct foreign-based access to, CPNI is permitted, and that, with foreign access, the FCC's preemption is, in fact, not certain nor clearly dispositive.

<sup>3</sup> MLATs, which are negotiated and implemented by the U.S. Department of State and Department of Justice, are carefully crafted to secure U.S. interests in acquiring information, records, etc. that are maintained in a foreign country. Because of their reciprocal nature, they also provide substantive and procedural safeguards for the security and privacy of information and records of U.S. Governmental and business entities and of U.S. citizens that are maintained in the U.S. against unwarranted foreign government access. For example, MLATs provide foreign governments access to a telephone subscriber's CPNI (subscriber information and records), etc., only upon an appropriate investigative, prosecutive, or other lawful request, based on legitimate need, demonstrated by the requesting foreign government, and concurred in by appropriate U.S. executive and (or) judicial branch entities. As part of the U.S.-based disposition of a foreign request is a finding of whether it is consistent with U.S. law and interests. Like all treaties, MLATs must be ratified by the U.S. Senate.

## Historic Treatment of CPNI

Historically, the FCC appears to have treated CPNI, in many regards, as *carrier proprietary* information, rather than as *customer proprietary* information, which information the carrier could utilize in its network for call placement, billing, etc., but also for a broad range of carrier uses. Further, the FCC has recognized CPNI as being an important component in a carrier's establishing or controlling its market power. Hence, in recent years, one of the greatest points of FCC emphasis regarding CPNI appears to have been with regard to the matter of incumbent and competitor access to subscriber CPNI, with FCC treatment designed to foster competition. However, the very significant latitude that carriers have with regard to the uses and physical handling of their customers' CPNI has received less attention<sup>4</sup> -- with uses, handling, and storage of CPNI being largely unrestrained, for example, by any requirement of prior consent or authorization for many telephone customers or by law enforcement-based requirements or conditions.<sup>5</sup> But, as is increasingly being recognized, electronic access to (and handling, storage, and disclosure of) subscriber CPNI (particularly subscriber information and dialing/billing records) undoubtedly also implicate important customer privacy and proprietary interests, as well as important governmental (law enforcement, public safety, and national security) interests. CPNI comprehends detailed and sensitive proprietary information about a customer's use of network services; his/her calling patterns; social, medical, organizational, and political telephone contacts; and much more. Thus, nonconsensual access to and disclosure of such information should be grounded in legitimate need, such as is required for law enforcement access (discussed below). Moreover, as discussed in this Comment, it is also essential that the practical aspects and implications of direct physical access to Domestic Customer CPNI through foreign-based storage of CPNI, and direct foreign-based electronic access to CPNI, be seriously addressed by the FCC -- above and beyond the purely legal or competitive-regulatory aspects of carrier use, access, and disclosure of a customer's CPNI. This FCC consideration is essential since such foreign-

---

<sup>4</sup> The FBI notes prior FCC competitively-grounded efforts to protect CPNI (restricting computer access to CPNI, to prevent carrier enhanced services and CPE personnel access). However, as discussed below, CPNI privacy considerations are hardly satisfied by computer access protections exclusively, especially where foreign-based access is involved.

<sup>5</sup> The Telecommunications Act of 1996 has taken an important step in recognizing the significance of customer proprietary information. Section 702. While this law is useful in stating the proposition that the privacy rights of telephone subscribers is important and that CPNI should be limited to particular uses (see section 702, under the amendment to, and in the newly-created section 222 (c)(1) and (2) of, the Communications Act of 1934), it does not speak to the important issue of where customer proprietary information may be stored or from where it might be accessed. This latter point, we believe, has a direct and an extremely significant impact upon the underlying goal of customer privacy. Moreover, as discussed in this Comment, there are other substantial governmental, business, and societal concerns interrelated with the concern of customer privacy. The FBI strongly urges the FCC to incorporate these concerns into its analysis and the instant rulemaking endeavor.

based storage of, and access to, Domestic Customer CPNI has the clear potential of undermining FCC rules and regulations as well as other U.S.-privacy-based laws.<sup>6</sup>

### **The FBI's Interest in the CPNI Docket**

The FBI, along with the U.S. Department of Defense (DoD), recently concluded a series of meetings with MCI Communications Corporation (MCI) and British Telecommunications plc (BT) incidental to the proposed MCI and BT merger and the application to transfer MCI's current licenses to a new, to-be-created parent company, Concert plc ("Concert"), the majority ownership of which would be British (GN Docket No. 96-245). In these meetings, the matter of foreign-based storage of, and direct foreign access to, the CPNI of U.S. Domestic Customers arose. For many of the reasons discussed herein, the FBI and DoD expressed their concerns at that time.<sup>7</sup> Ultimately, the FBI and DoD concluded that the nature of their concerns was not peculiar to the MCI-BT merger, or even to foreign-based ownership of U.S. carriers generally, but rather that these concerns had applicability to all carriers licensed in the U.S. Consequently, it was mutually agreed among all of the parties that the resolution of this CPNI concern was best resolved before the FCC in a docket dedicated to the topic of the appropriate uses and handling of CPNI. In the interim, MCI-BT agreed, in essence, to a *standstill* regarding the matter of foreign storage of, and access to, the CPNI of their Domestic Customers, pending the resolution of this CPNI issue by the FCC (with the standstill running until the earlier of March 31, 1998, or the effective date of any FCC regulations specifically related to and resolving this particular issue).

### **Law Enforcement and Public Safety Concerns**

The FBI and the U.S. law enforcement community have a strong and distinct law enforcement and public safety interest in the CPNI of Domestic Customers being

---

<sup>6</sup> It is the opinion of the FBI that the FCC has never been called upon to formally consider, for example, the privacy, business, law enforcement, public safety, and national security implications of permitting FCC-licensed carriers to physically store U.S. Domestic Customer CPNI outside of the U.S. or of permitting such CPNI, although stored in the U.S., to be directly accessible electronically from a foreign country. As a practical matter, the FCC may never have been called upon to issue regulations regarding this important issue since until recently it may have been chiefly a theoretical concern. However, with the increased prospect of foreign-based ownership and operation of U.S. carriers, and the increase in mergers, joint ventures, etc. with U.S. carriers, the immediacy of the concern regarding foreign-based storage of, or direct foreign access to, U.S. Domestic Customer CPNI is both real and palpable.

<sup>7</sup> The Comments expressed here are those of the FBI, but we believe that they also encompass concerns of law enforcement generally regarding this CPNI issue.

exclusively stored in, and accessible solely from within, the U.S.<sup>8</sup> The law enforcement community, in the course of criminal and other investigations, routinely requires prompt, secure, and confidential access to customer subscriber information and records. Such subscriber information and records constitute the vast majority of the CPNI that carriers maintain. In virtually every federal, state, or local investigation of consequence, telephone subscriber and/or toll or billing records are obtained.<sup>9</sup> Frequently, information derived therefrom not only becomes critical evidence in trials, but it is also often critical to law enforcement in saving lives.<sup>10</sup> In all such cases, U.S. law enforcement agencies acquire this type of information pursuant to lawful authority.<sup>11</sup>

Requiring that the CPNI of U.S. Domestic Customers exclusively be stored in, or exclusively be accessible from within, the U.S. is essential for a number of compelling law enforcement and public safety reasons, including the following:

- 1) it facilitates the U.S. law enforcement and public safety imperative that there shall be prompt and sure, and secure and confidential, access to such information in the U.S.;
- 2) it obviates the need for U.S. law enforcement agencies to have to needlessly resort to burdensome, time-consuming, and uncertain international processes

---

<sup>8</sup> In this Comment, the FBI's central concern relates to the issue of foreign-based storage of, or direct foreign electronic access to, the CPNI of *Domestic Customers*. The FBI believes that the FCC should mandate that the CPNI of Domestic Customers shall be exclusively stored in (accessible from) the U.S. However, even with regard to U.S.-based customers who fall outside this category (*see footnote 1, supra*), it is imperative that a copy of those customers' CPNI

be stored in the U.S. because of the critical need for prompt, secure, and confidential law enforcement, public safety, or national security access to such information, pursuant to lawful authority.

<sup>9</sup> In response to critical law enforcement investigative and public safety needs, the FCC established in regulation the requirement that common carriers retain telephone toll records for a period of 18 months. 47 C.F.R. Sec. 42.6 (1996). The imperative for the availability of, and for prompt law enforcement access to, subscriber records and other potential evidence related to subscribers, particularly in terrorism cases, was recently underscored by the Congress. Under section 804 of the "Antiterrorism and Effective Death Penalty Act of 1996" (Pub.L. 104-132, codified at 18 U.S.C. 2703(f)), carriers and others, upon the request of a governmental entity, are mandated to "take all necessary steps to *preserve* records and other evidence in [their] possession *pending the issuance of a court order or other process.*" (emphasis added).

<sup>10</sup> The prompt acquisition of telephone subscriber information, whether obtained as a record (or acquired in a more "real time" fashion through pen register devices or traps and traces) is essential to effective law enforcement and the public safety. Such information has been essential in saving hundreds of lives in kidnaping, extortion, and homicide investigations, and in effecting the speedy apprehension of dangerous and violent felons.

<sup>11</sup> *See, e.g.,* 18 U.S.C. 2703(c) and similar legal process required under state law.

such as MLATs or Letters Rogatory to obtain purely domestic U.S. CPNI information related to purely domestic U. S. investigations;

3) it very substantially reduces the possibility of domestic investigations being compromised by foreign personnel, particularly where the criminal or terrorist investigations, etc. may relate to the same foreign government or its agents, its corporations, organizations, etc. (e.g., foreign, state-sponsored or tolerated terrorists, or international-based criminal enterprises, including organized crime families and drug-trafficking cartels) where the CPNI is stored or from where it is accessible; and

4) it would prevent the prospect of *U.S. domestic-based* criminals and terrorists from purposely attempting to seek out, and establish arrangements with, U.S.-licensed carriers to “create” *foreign “safe-havens”* for the storage of their CPNI -- that is, intentionally putting Domestic Customer CPNI effectively out of the reach of U.S. law enforcement entities either altogether, or, at a minimum, undercutting timely and confidential law enforcement access thereto. (Moreover, such foreign storage and access would permit foreign-based alteration or manipulation of the CPNI.)

Given the foregoing reasons, there appears to be an extremely strong and compelling justification for the FCC to require carriers licensed in the U.S. to store the CPNI of U.S. Domestic Customers exclusively within the U.S. (and to solely permit direct electronic access to it from within the U.S.), based upon vital law enforcement and public safety concerns.

### **National Security and Espionage Concerns**

The FBI and the U.S. intelligence community have a strong and distinct national security interest in the CPNI of U.S. Domestic Customers being exclusively stored in, and accessible solely from within, the U.S.<sup>12</sup> The FBI and the intelligence community, in the course of intelligence-based, foreign counterintelligence, international terrorism, and espionage investigations, routinely require prompt, secure, and confidential access to the subscriber information and records of Domestic Customers. Such subscriber information and records may well constitute the vast majority of the CPNI that carriers maintain. In virtually every intelligence-based, foreign counterintelligence, international terrorism, and espionage

---

<sup>12</sup> As noted in footnote 5, *supra*, this FBI Comment principally relates to the issue of foreign-based storage of, and direct foreign electronic access to, the CPNI of U. S. *Domestic Customers*. However, even with regard to U.S.-based customers who fall outside this category (*see footnote 1, supra*), it is imperative that a *copy* of those customers' CPNI be stored in the U.S. because of the critical necessity for prompt, secure, and confidential law enforcement, public safety, or national security access to such information pursuant to lawful authority.

investigation of consequence, telephone subscriber and/or toll or billing records are obtained.<sup>13</sup> Frequently, information derived therefrom is not only vital in properly conducting national security-based investigations, but it also often produces critical evidence in international terrorism and espionage trials, and, importantly, has enabled law enforcement and national security agencies to prevent terrorist acts and acts of espionage.<sup>14</sup> In all such cases, the FBI and intelligence agencies acquire this type of information pursuant to lawful authority.<sup>15</sup>

Requiring that the CPNI of U.S. Domestic Customers exclusively be stored in, or exclusively be accessible from within, the U.S. is essential for a number of compelling national security-based reasons, including the following:

- 1) it facilitates the U.S. national security and intelligence imperative that there shall be prompt and sure, secure and confidential, access to such information in the U.S.;
- 2) it obviates the need for U.S. intelligence agencies to have to needlessly resort to burdensome, time-consuming, and uncertain international processes such as MLATs or Letters Rogatory to obtain purely domestic U.S. CPNI information related to purely domestic U.S. investigations;<sup>16</sup>

---

<sup>13</sup> As noted in footnote 6, *supra*, in response to critical law enforcement investigative and public safety needs, the FCC established in regulation the requirement that common carriers retain telephone toll records for a period of 18 months. 47 C.F.R. Sec. 42.6 (1996). The significance of subscriber records and other potential evidence related to subscribers, particularly in terrorism cases, was recently underscored by the Congress. Under section 804 of the "Antiterrorism and Effective Death Penalty Act of 1996" (Pub.L. 104-132, codified at 18 U.S.C. 2703(f)), carriers and others, upon the request of a governmental entity, are mandated to "take all necessary steps to *preserve* records and other evidence in [their] possession *pending the issuance of* a court order or other process." (emphasis added).

<sup>14</sup> The prompt acquisition of telephone subscriber information, whether obtained as a record (or acquired in a more "real time" fashion through pen register devices or traps and traces) is essential to effective national security-based investigations. Such information has been essential in saving lives in international terrorism cases and in preventing grave damage (either altogether or in preventing ongoing damage) to the national security interests of the U.S. through espionage efforts.

<sup>15</sup> See, e.g., 18 U.S.C. 2709, and access pursuant to 50 U.S.C. 1801 *et seq.*

<sup>16</sup> It is extremely important to note that, generally speaking, MLATS and Letters Rogatory, etc., are applicable to criminal investigations. Hence, requests to foreign governments for information or records related to espionage, international terrorism, or intelligence-based investigative information may, in most cases, be precluded altogether under such treaties or procedures. Being precluded from obtaining such CPNI would be intolerable from a national security perspective. Even if available, requests to a foreign country for CPNI pertaining to the telephone service, records, or subscriber information of its own intelligence agencies or agents or home-grown terrorists would be ludicrous. Even where such investigations related to subjects associated with another foreign country, requests to foreign countries, practically speaking, would be precluded since the



3) it very substantially reduces the possibility of domestically-grounded national security-based investigations being compromised by foreign personnel, particularly where the espionage, international terrorism, or intelligence-based investigation may relate to the same foreign government or its agents, organizations, etc. (e.g., foreign, state-sponsored or tolerated international terrorists, or foreign intelligence officers) where the CPNI is stored or from where it is accessible;

4) it would prevent the prospect of *U.S. domestic-based* foreign spies and international terrorists from purposely attempting to seek out, and establish arrangements with, U.S. licensed carriers in order to "create" *foreign "safe-havens"* for storage of their CPNI -- that is, intentionally putting Domestic Customer CPNI effectively out of the reach of U.S. intelligence agencies either altogether, or, at a minimum, undercutting timely and confidential national security-based access thereto; and

5) it would prevent foreign-based personnel, including foreign intelligence officers from having direct access to the Governmental office, mobile, and home telephone subscriber and dialing/billing record information of officials and employees of the U.S. Government (especially those who hold positions in the defense, intelligence, national security, and diplomatic arenas) for the purposes of determining their official, governmental telephone contacts <sup>17</sup> and their personal telephone contacts.<sup>18</sup>

---

underlying legal process and information typically would be classified and execution of the request abroad would almost certainly be precluded, infeasible, or unacceptable.

<sup>17</sup> It is manifestly obvious that it would be extremely improper for the governmental office or car telephone service activity (CPNI), or the home or private car telephone service activity (CPNI) of, for example, the Director of the FBI, the Secretary of Defense, the Secretary of State, or the Director of Central Intelligence, etc. to be stored abroad or to be directly accessible from abroad (effectively, at the finger tips of foreign intelligence agents). Moreover, it would be life-threatening, for example, for such telephone service information (CPNI) of FBI undercover agents who are working foreign international terrorism cases to have their CPNI stored abroad or to be directly accessible from abroad. The FBI has also received information that foreign carrier personnel, monitoring the CPNI of drug enforcement officials overseas (and, in particular, with regard to their contacts with informants), have passed this information about informant contacts to drug cartel leaders, the result of which was the murder of suspected informants.

<sup>18</sup> The CPNI of governmental officials may well disclose telephone contacts which would suggest to a foreign intelligence officer that the U.S. official could be "recruited," "blackmailed," or "compromised." For example, a U.S. official's contacts with banks, credit bureaus, etc.; counseling agencies or alcohol or drug counseling entities; sexual liaison contacts; etc. could give a foreign power the intelligence and leverage needed to recruit the U.S. official, leading to espionage and other grave national security harm.

Given the foregoing reasons, there appears to be an extremely strong and compelling justification for the FCC to require carriers licensed in the U.S. to store the CPNI of U.S. Domestic Customers exclusively within the U.S. (and to solely permit direct electronic access to it from within the U.S.), based upon vital national security and intelligence-based concerns.

### **Economic Espionage and Access to Proprietary Business Information**

The FBI is charged with investigating economic espionage. The Congress has recently recognized the extreme harm that can result to vital U.S. economic, competitive, and economic-security interests as a result of economic espionage, particularly with regard to economic espionage conducted by foreign spies, intelligence officers, etc.<sup>19</sup> Aside from investigating acts of economic espionage, the FBI also seeks to prevent economic espionage from occurring in the first instance. In addition to the coordinated government-wide response effort conducted through the National Counterintelligence Center located at CIA Headquarters and led by an FBI Special Agent, the FBI carries out economic espionage alerts and guidance to U.S. industry through its Awareness of National Security Issues and Response (ANSIR) (formerly, the Development of Espionage, Counterintelligence and Counterterrorism Awareness (DECA)) program. The Department of State also conducts a program similar to ANSIR (DECA) to alert U.S. businesses overseas to foreign economic espionage threats.

The ready availability of U.S. Domestic Customer CPNI (through foreign-based storage or direct electronic foreign access) would be of great aid to foreign spies, intelligence officers, and their agents in conducting economic espionage. As noted above, CPNI comprehends detailed and sensitive proprietary information about a business customer's use of network services; his/her calling patterns; client and sales contacts; contractual relationships, and many other business-sensitive and proprietary contacts; and much more. Thus, nonconsensual carrier disclosure of Domestic Customer CPNI should be tied to lawful access exclusively under U.S. law. Further, foreign storage or direct electronic foreign access should never be permitted to occur absent clear, affirmative, and informed *written* customer consent.<sup>20</sup> At base, the matter of (threat posed by) foreign-based

---

<sup>19</sup> See, e.g., the "Economic Espionage Act of 1996," Pub.L. 104-294, Title I, Sec. 101(a), 110 Stat. 3488 (codified at 18 U.S.C. 1831-39), including 142 Cong. Rec. S12207 and S12211 (daily ed. Oct. 2, 1996) (statements of Sens. Specter and Kohl, respectively). See also, the "National Information Infrastructure Act of 1996," Pub.L. 104-294, Title II, Sec. 201, 110 Stat. 3491 (codified at 18 U.S.C. 1030), including 142 Cong. Rec. S12214 (daily ed. Oct. 2, 1996) (statement of Sen. Leahy) (related to protections against the unauthorized accessing of, or exceeding authorized access to, information from protected computers where the conduct involves an interstate or foreign communication).

<sup>20</sup> This observation may have its greatest relevance with regard to unwary business subscribers whose business-proprietary CPNI may lend itself to the prospect of foreign-based economic espionage. However, the basis and logic for a requirement mandating clear, explicit, and affirmative consent applies to all types of

physical and technical access to Domestic Customer CPNI is, practically speaking, as important as the legal or regulatory conditions otherwise imposed upon carrier access or disclosure of CPNI through the FCC's rulemaking or otherwise by U.S. law. Foreign-based storage of, or direct foreign electronic access to, Domestic Customer CPNI would undermine reasonable subscriber assumptions about the safety, security, and business-proprietary and privacy protections that normally would be expected to exist under U.S. law.<sup>21</sup>

Thus, the FBI believes that there are strong and distinct economic-security interests in requiring the CPNI of Domestic Customers to be exclusively stored and maintained in the U.S.

Requiring that the CPNI of U.S. Domestic Customers exclusively be stored in, or exclusively accessible from within, the U.S. is essential for a number of compelling economic, business-proprietary, and economic-security reasons, including the following:

- 1) it facilitates the U.S. economic security imperative that there would only be secure and lawful access to U.S. Domestic Customer CPNI information in the U.S., and only under U.S. law;
- 2) it facilitates the business-proprietary and privacy imperative that there would only be secure and lawful access to U.S. Domestic Customer CPNI information in the U.S., and only under U.S. law;
- 3) it would prevent foreign-based personnel, including foreign intelligence officers, from having direct access to the business office, mobile, and home telephone service activity and subscriber and dialing/billing record information (CPNI) of U.S. corporate and business leaders and their employees for the purposes of determining their business-related telephone contacts; and

---

subscribers -- businesses, Governmental, and individuals. For Governmental CPNI or a business or private person's CPNI to be stored in a foreign country or directly accessible from a foreign country, the subscriber's consent should be unmistakably explicit and in writing (i.e., "I, [customer], hereby authorize Carrier X to store my CPNI in [country Y] and/or to permit direct foreign electronic access to my CPNI from [country Y].") As noted above, even if a Domestic Customer or other carrier customer explicitly consented in writing to foreign access to its CPNI, the FCC, for the public safety, law enforcement, and national security reasons set forth herein, should nonetheless require carriers to maintain a *copy* of such CPNI in the U.S. because of the imperative that such information must be promptly available pursuant to lawful authority.

<sup>21</sup> Indeed, permitting certain carriers to store the CPNI of Domestic Customers abroad, or permitting access to it from abroad, would, as a practical matter, constitute FCC endorsement of the paradigm that certain customers can properly be accorded disparate, and greatly-reduced privacy protections, thereby creating a two-tiered regime, wherein there is created "second-class citizen" CPNI telecommunications privacy rights. Thus, notions of market "dominance," effective competitive opportunities, or other competition or trade-based criteria should not be allowed to depreciate any subscriber's CPNI. Moreover, protection of a subscriber's CPNI should not be dependent upon whether the subscriber's carrier is foreign- owned, influenced, or controlled.

4) it would prevent foreign-based personnel, including foreign intelligence officers, from having direct access to the personal home telephone or mobile telephone service activity and subscriber and dialing/billing record information of U.S. corporate and business leaders and their employees for the purpose of determining their personal telephone contacts.<sup>22</sup>

Given the foregoing reasons, there appears to be an extremely strong and compelling justification for the FCC to require carriers licensed in the U.S. to store the CPNI of U.S. Domestic Customers exclusively within the U.S. (and to solely permit direct electronic access to it from within the U.S.), based upon very important economic security and business-proprietary-based concerns.

### **Subscriber CPNI Privacy Concerns**

The FBI believes that there are strong and distinct subscriber privacy interests involved in ensuring that the CPNI of Domestic Customers is exclusively stored in, and accessible solely from within, the U.S. Subscriber dialing and billing information and records constitute the vast majority of the CPNI that carriers maintain. CPNI comprehends detailed, sensitive, and often highly-personal information about a customer's use of network services; his/her calling patterns; social, medical, organizational, and political telephone contacts; and much more. Thus, nonconsensual access to and disclosure of such information should be grounded in legitimate need, such as is required for law enforcement access. Foreign-based storage of or access to U.S. Domestic Customer CPNI, since it would be unconstrained by U.S. law, poses distinct threats to the privacy of U.S. persons and would undermine subscriber privacy expectations and assumptions that exist when their CPNI is maintained exclusively in the U.S. The FBI believes that the FCC should consider the *realities* that would come into play, in terms of foreign government and foreign private sector access to the CPNI of U.S. Domestic Customers, if such access were allowed to occur. Foreign laws (if any) notwithstanding, the historic practices of foreign-based telephone personnel (including their employment with government-owned (operated or controlled) telephone companies and their and their company's interrelationships with the host foreign government and major host country corporations) have not been those required of or demonstrated by U.S.-based telephone personnel.

### **Past FCC Safeguards**

---

<sup>22</sup> The CPNI of corporate and business officials and their employees may well disclose telephone contacts which would suggest to a foreign intelligence officer that the U.S. business person could be "recruited," "blackmailed," or "compromised." For example, a U.S. business person's contacts with banks, credit bureaus, etc.; counseling agencies or alcohol or drug counseling entities; sexual liaison contacts; etc. could give a foreign power the intelligence and leverage needed to recruit the U.S. business person, leading to economic espionage, and perhaps to traditional espionage if the business employee was working on classified government contracts.

## Regarding CPNI

The FBI believes that the CPNI of U.S. Domestic Customers (Governmental, business, and private customers) must be aggressively protected. The FCC appears to have recognized that certain precautions, such as preventing access to CPNI by enhanced service and CPE personnel, may preclude competitive disadvantages, and also arguably enhance customer privacy. Such practices and others within the U.S. should continue, with auditing required to ensure that access to CPNI is proper and necessary. U.S. law enforcement community access to CPNI has been carefully prescribed under U.S. law for some time, a circumstance that the law enforcement community respects and follows. It makes little sense, however, in terms of privacy, to permit widespread physical or electronic access to CPNI, with few, if any, physical constraints and technical gateways being employed by carriers. Moreover, we believe that sensitive CPNI should not be protected solely through reliance upon prohibitions stated in law or regulation -- physical and technological controls and audit procedures should also be employed to ensure that laws and regulations are *enforceable*.

Beyond the measures suggested above, it is imperative that the FCC recognize that even physical and technical measures will be of little or no avail if foreign storage of, or foreign direct electronic access to, U.S. Domestic Customer CPNI is permitted. Aside from the impact of foreign law and unofficial foreign practices in undoing potential protections which FCC regulations may specify or which other U.S. law may require, past hostile practices and efforts by some foreign governments and their agents to monitor U.S. subscriber activity is well recognized and will not cease, regardless of whether the personnel are employed by a U.S.-based company or otherwise.<sup>23</sup>

## Conclusion

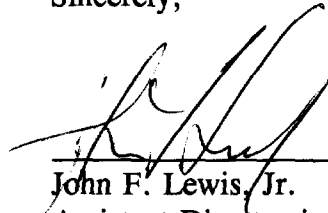
The FBI believes, based upon vital law enforcement, public safety, national security, business-proprietary, and personal privacy customer concerns, that there are compelling reasons and strong justifications for the FCC to impose constraints on FCC-licensed telecommunications carriers by enjoining them from storing Domestic Customer CPNI outside the United States and enjoining any capability that may exist that permits access, from outside the U.S., to Domestic Customer CPNI that is stored in the U.S. The FBI believes that the concerns regarding foreign-based storage of, or direct foreign electronic access to, the CPNI of Domestic Customers logically apply to all carriers since the harm to be avoided with regard to U.S. Governmental and customer interests is essentially identical regardless of whether the carrier is U.S. or foreign-based. These concerns also logically apply without regard to the "dominance," size, or the competitive circumstances of the

---

<sup>23</sup> The efforts of foreign-based personnel to acquire intelligence about a variety of U.S. Governmental and business entities and persons has been documented in the book **Friendly Spies How America's Allies Are Using Economic Espionage to Steal Our Secrets** by Peter Schweizer, The Atlantic Monthly Press (New York 1993).

carriers. Foreign-based storage of, or direct foreign access to, the CPNI of Domestic Customers would undermine the efficacy of FCC regulations and other U.S. laws related to CPNI, particularly with regard to vital national security, law enforcement, public safety, business-proprietary, and privacy concerns. If foreign storage of, or direct foreign access to, such CPNI is permitted, FCC jurisdictional, enforcement, audit, and inspection capabilities regarding foreign carrier facilities and activities would be extremely doubtful, practically and legally. The reality would be that foreign laws and (or) foreign practices would effectively supersede any provisions of U.S. law, including those normally associated with FCC preemption, related to CPNI. Moreover, the prospect of direct foreign access to the CPNI of U.S. Domestic Customers would have the unintended effect of seriously undermining important U.S. Governmental, business-proprietary, and privacy-based protections that are afforded to CPNI under international and bilateral treaties (such as MLATs) and other international legal assistance procedures.

Sincerely,

  
\_\_\_\_\_  
John F. Lewis, Jr.

Assistant Director in Charge  
National Security Division  
July 8, 1997